

# **CIPHER RECORDER, CIPHER RECORDING METHOD, PROGRAM FOR MAKING COMPUTER CARRY OUT THE METHOD, AND COMPUTER READABLE RECORDING MEDIUM WITH THE PROGRAM RECORDED THEREON**

Publication number: JP2002313020 (A)

Also published as:

Publication date: 2002-10-25

☐ JP3786015 (B2)

Inventor(s): OSHIMA MITSUAKI; GOTOU YOSHITOSHI; TANAKA SHINICHI; KOISHI KENJI; MORIYA MITSURO; TAKEMURA YOSHIYA +

Applicant(s): MATSUSHITA ELECTRIC IND CO LTD +

Classification:

- International: G06F12/14; G06F21/24; G11B20/10; G11B7/004; H04L9/32; G06F12/14; G06F21/00; G11B20/10; G11B7/00; H04L9/32; (IPC1-7): G06F12/14; G11B20/10; G11B7/004; H04L9/32

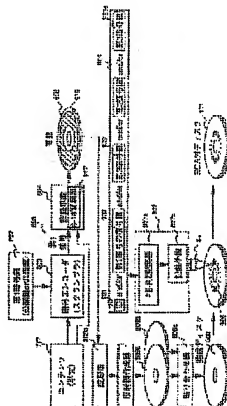
- European:

Application number: JP20020008404 20020117

Priority number(s): JP20020008404 20020117; JP19950261247 19951009; JP19960008910 19960123; JP19960211304 19960809

## **Abstract of JP 2002313020 (A)**

**PROBLEM TO BE SOLVED:** To simplify operation sequence or procedures for the applied system of a network using type optical disk. **SOLUTION:** A sub-information recording area is provided to the optical disk, and an ID or a cryptographic key or a decoding key different from a disk to a disk is recorded at a factory. Operation sequence or procedures can be obviated by a user's using the ID for deciphering software, the cryptographic key when transmitting a cipher, the decoding key when receiving a cipher, and safe distribution of information via a communication means is realized by checking the record of contents using prescribed information.



Data supplied from the *espacenet* database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-313020

(P2002-313020A)

(43)公開日 平成14年10月25日(2002.10.25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	データベース(参考)
G 1 1 B 20/10		C 1 1 B 20/10	H 5 B 0 1 7
G 0 6 F 12/14	3 2 0	C 0 6 F 12/14	3 2 0 B 5 D 0 4 4
			3 2 0 F 5 D 0 9 0
G 1 1 B 7/004		G 1 1 B 7/004	C 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 B

審査請求 有 請求項の数10 ○L (全 30 頁)

審査請求 有 請求項の数10 O.L (全 30 頁)

(21) 出願番号	特願2002-8404(P2002-8404)
(62) 分割の表示	特願平9-511086の分割
(22) 出願日	平成8年10月8日(1996.10.8)
(31) 優先権主張番号	特願平7-261247
(32) 優先日	平成7年10月9日(1995.10.9)
(33) 優先権主張国	日本(JP)
(31) 優先権主張番号	特願平8-8910
(32) 優先日	平成8年1月23日(1996.1.23)
(33) 優先権主張国	日本(JP)
(31) 優先権主張番号	特願平8-211304
(32) 優先日	平成8年8月9日(1996.8.9)
(33) 優先権主張国	日本(JP)

(71)出願人 000003821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地

(72)発明者 大嶋 光昭  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 後藤 芳稔  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74)代理人 10009/445  
弁理士 岩橋 文雄 (外2名)

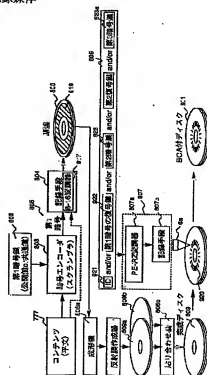
## 最終頁に書く

(54) 【発明の名称】 暗号記録装置、暗号記録方法、その方法をコンピュータに実行させるプログラムおよびそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 ネットワーク利用型の光ディスクの応用システムの操作手順や諸手続きを簡便化する。

【解決手段】 光ディスクに副情報記録領域を設け、ディスク毎に異なるIDや暗号の暗号鍵や復号鍵を工場で記録しておく、使用者がソフトの暗号解除にはID、暗号送信時に暗号鍵、暗号受信時に復号鍵を用いることにより手順や手続きを省略でき、コンテンツの記録を所定の情報を用いたチェックを行うことで通信手段を介して安全な情報配信が実現する。



## 【特許請求の範囲】

【請求項1】 コンテンツを入力するための入力手段と、

入力された前記コンテンツを暗号化する暗号化手段と、暗号化された前記コンテンツを記録する記録手段と、を備え、

前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行い、そのチェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。

【請求項2】 コンテンツを受信する受信手段と、受信された前記コンテンツを暗号化する暗号化手段と、暗号化された前記コンテンツを記録する記録手段と、を備え、

前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行い、そのチェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。

【請求項3】 コンテンツを入力するための入力手段と、

入力された前記コンテンツを暗号化する暗号化手段と、暗号化された前記コンテンツを記録する記録手段と、前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行うチェック手段と、を備え、

前記チェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。

【請求項4】 コンテンツを受信する受信手段と、受信された前記コンテンツを暗号化する暗号化手段と、暗号化された前記コンテンツを記録する記録手段と、前記暗号化手段と前記記録手段との間で、所定の情報を用いたチェックを行うチェック手段と、を備え、

前記チェックが正常な場合に、前記暗号化手段で暗号化された前記コンテンツが前記記録手段に送られることを特徴とする暗号記録装置。

【請求項5】 前記所定の情報は、暗号化された前記コンテンツが記録される記録媒体に格納された情報であることを特徴とする請求項1から4の何れか1項に記載の暗号記録装置。

【請求項6】 前記所定の情報は、暗号化された前記コンテンツが記録される記録媒体を識別する識別情報であることを特徴とする1から4の何れか1項に記載の暗号記録装置。

【請求項7】 コンテンツを入力する入力工程と、入力された前記コンテンツを暗号化する暗号化工程と、

前記暗号化を行う暗号化手段と暗号化された前記コンテンツを記録する記録手段との間で、所定の情報を用いたチェックを行うチェック工程と、

前記チェックが正常な場合に、暗号化された前記コンテンツを記録する記録工程と、を含むことを特徴とする暗号記録方法。

【請求項8】 コンテンツを受信する受信工程と、受信された前記コンテンツを暗号化する暗号化工程と、前記暗号化を行う暗号化手段と暗号化された前記コンテンツを記録する記録手段との間で、所定の情報を用いたチェックを行うチェック工程と、

前記チェックが正常な場合に、暗号化された前記コンテンツを記録する記録工程と、を含むことを特徴とする暗号記録方法。

【請求項9】 請求項7または8に記載の暗号記録方法をコンピュータに実行させるプログラム。

【請求項10】 請求項9に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は光ディスクおよび光ディスクシステムおよび暗号通信方法に関するものである。

【0002】

【従来の技術】近年、インターネット等のネットワークと光ROMディスクの普及に伴い、光ROMディスクを用いたネットワークソフト流通が始まりつつある。また電子商取引の検討が進んでいる。

【0003】従来技術として、CD-ROMをメディアとして用いたソフト電子流通システムが実用化されている。この場合パスワードを与えて、CD-ROMに予め記録された暗号化されたソフトの暗号を解くといった方法が一般的である。

【0004】

【発明が解決しようとする課題】しかし、CD-ROMの場合、ディスク上に追記記録できないため各ディスクのIDは個別に設定できない。従って単純に用いば、1つのパスワードが同一原盤から製造された全てのディスクの暗号を解除してしまう。このため、CD-ROMを用いた場合、各々のディスク固有のIDをパソコン側のハードディスク上に作成したり、センターで作成したIDを郵便によりユーザーに送るという作業が必要であった。

【0005】従来の光ディスクや光ディスクシステムを用いた電子流通システムにおいては、光ディスクもしくはシステムにIDや暗号鍵を簡便に供給することが求められている。本発明はROMディスクを用いた電子流通システムにIDと暗号鍵の簡便な供給を実現することを目的とする。

【0006】

【課題を解決するための手段】この課題を解決するために、光ディスクのビット部にバーコードを重ね書きした追記領域（以下BCAと略す）を設け光ディスク製造時

に、BCA領域にディスク毎に異なるIDと必要に応じて通信用の暗号鍵、通信用の復号鍵略号文の復号鍵を個別に記録しておくことにより、ディスクとユーザーに配布した時点で、ユーザーにはユーザーID番号と通信用の送信用の暗号鍵、受信用の復号鍵の3つが自動的に配布されていることになり、従来のシステムを複雑にしていたいくつかの手順が省略できる。こうして、暗号通信とコンテンツの入ったディスクの識別が同時に実現する。

#### 【0007】

【発明の実施の形態】実施例に基づき、本発明を説明する。なお、本文ではBCA方式を用いた追記領域をBCA領域、BCAにより記録されたデータをBCAデータと呼ぶ。また第1識別情報はID、もしくはディスクIDとも呼ぶ。

【0008】図1はBCA付ディスクの代表的な工程を示す。まず、公開鍵等の第1暗号鍵802を用いて暗号エンコード803でコンテンツ777が暗号化された第1暗号805がマスタリング装置等の8-16変調器917により変調され、この変調信号がレーザーにより原盤800の第1記録領域919に凹凸のビットとして記録される。この原盤800を用いて成形機808aでディスク状の透明基板918を成形し、反射膜作成機808bでA1反射膜を形成し0.6ミリの厚の片面ディスク809a、809bを作成し、貼り合わせ機808cで貼り合わせた完成ディスク809の第2記録領域920にトリミング装置807で、ディスクID921もしくは第1暗号の復号鍵922もしくはインターネット通信用の第2暗号鍵923をPE変調とRZ変調を組み合わせたPE-RZ変調器807aで変調し、パルスレーザ-807bでBCAトリミングして、BCA付ディスク801を製造する。貼り合わせディスクを用いているので、中に入ったBCAは改ざん出来ず、セキュリティ用途に用いることができる。

【0009】説明に入る前に、BCAについて、簡単に説明する。

【0010】図2の(1)に示すようにBCAでは2層ディスク800にパルスレーザ-808で、アルミ反射膜809をトリミングし、ストライプ状の低反射部810をPE変調信号に基づいて記録する。図2(2)に示すようにBCAのストライプがディスク上に形成され、このストライプを通常の光ヘッドで再生するとBCA部は反射信号がなくなるため図2(3)に示すように変調信号が間欠的に欠落した欠落部810a、810b、810cが発生する。変調信号は第1スライスレベル915でスライスされる。一方欠落部810a等は信号レベルが低いので、第2スライスレベル916で容易にスライスできる。図3の記録再生波形図に示す様に、形成されたバーコード923a、923bは、図3(5)に示すように通常の光ビックで第2スライスレベル916で

レベルスライスすることにより再生可能で図3(6)に示すようにLPFフィルタで波形成形されPE-RZ復調され、(7)に示すようにデジタル信号が出力される。図4を用いて復調動作を説明する。まず、BCA付ディスク801は透明基板が2枚、記録層801aが中にくるように貼り合わせてあり、記録層801aが1層の場合と記録層801a、801bの2層の場合がある。2層の場合は光ヘッド6に近い第1層の記録層801aのコントロールデータにBCAが記録されているかどうかを示すBCAフラグ922が記録されている。BCAは第2層801bに記録されているので、まず第1層記録層801aに焦点を合わせ第2記録領域919の最内周にあるコントロールデータ924の半径位置へ光ヘッド6を移動させる。コントロールデータは主情報なのでEFM又は8-15又は8-16変調されている。このコントロールデータの中のBCAフラグ922が'1'の時のみ、1層、2層部切換部827で、焦点を第2記録層801bに合わせBCAを再生する。レベルスライサ-590で図2(3)に示すような、一般的な第1スライスレベル915でスライスするとデジタル信号に変換される。この信号を第1復調部においてEFM925又は8-15変調926又は8-16変調927の復調器で復調し、ECCデコーダ36でエラー訂正し主情報が出力される。この主情報の中のコントロールデータを再生し、BCAフラグ922が1の場合のみBCAを読みにくい。BCAフラグ922が1の時、CPU923は1層、2層部切換部827に指示を出し、焦点調節部828を駆動して、第1層の記録層801aから第2層の記録層801bへ焦点を切り替える。同時に第2記録領域の920の半径位置、すなわちDVD規格の場合はコントロールデータの内周側の22.3mmから23.5mmの間に記録されているBCAを光ヘッド6を移動させ、BCAをよとめる。BCA領域では図2(3)に示すようなエンベロープが部分的に欠落した信号が再生される。第2レベルスライサ929において第1スライスレベル915より低い光量の第2スライスレベル916を設定することにより、BCAの反射部欠落部は検出でき、デジタル信号が出力される。この信号を第2復調部930においてPE-RZ復調し、ECCデコーダ930dにおいてECCデコードすることにより副情報であるBCAデータが出力される。このようにして、8-16変調の第1復調器928で主情報をPE-RZ変調の第2復調部930で副情報つまりBCAデータを復調再生する。

【0011】図5(a)にフィルタ943通過前の再生波形、(b)に低反射部810のスリットの加工寸法精度を示す。スリットの中は5~15μm以下にすることは難しい。また、23.5mmより内周に記録しないと記録データを破壊してしまう。このことからDVDの場合最短の記録周期=30μm、最大半径=23.5mm

mの制限からフォーマット後の最大容量は188bytes以下に限定される。

【0012】変調信号は、8-16変調方式を用いてビットで記録されており、図5(a)の高周波信号933のような高周波信号が得られる。一方、BCA信号は低周波信号932のような低周波信号となる。このように、主情報がDVD規格の場合、最高約4.5MHzの高周波信号932であり、図5(a)に示すように、副情報が周期8.92μsつまり約100KHzの低周波信号933であるため、LPF943を用いて副情報を周波数分離することが容易である。図4に示すようなLPF943を含む周波数分離手段934で、2つの信号を容易に分離することが出来る。この場合、LPF943は簡単な構成でよいという効果がある。

【0013】以上がBCAの概略である。

【0014】では、図6を用いて、暗号ソフト解錠システムの全体システムをパスワード発行と暗号通信と発注者の認証の動作に絞り説明する。まず、プレス工場のステップは、図1の場合とは同じ手順で製造されるので、原盤800と完成ディスク809の図は省略する。

【0015】プレス工場811において、第1～n番目のコンテンツの平文810は暗号エンコーダ812により、各々第1～n番目の暗号鍵813でデータの暗号化又は映像信号のスクランブルがなされ、光ディスクの原盤800に記録される。この原盤800から、プレスされて製造されたディスク状の基板809に反射膜が形成された後に、2枚のディスク状の基板を貼り合わせた後、完成ディスク809が作られる。この完成ディスク809に、ディスク毎に異なるID815もしくは/かつ第1暗号鍵816(公開鍵)もしくは/かつ、第2暗号鍵817(公開鍵)、第2コンピュータの接続アドレス818がBCA領域814に記録されたBCA付ディスク801が、ユーザーに配布される。

【0016】このディスクのコンテンツは暗号化されているので、再生するには代金等の代価を払ってパスワード発行センターつまり電子商店もしくは、モールからパスワードをもらう必要がある。この手順を述べる。

【0017】ユーザーの第1コンピュータ909では配布されたBCA付ディスク801を再生装置819で再生すると、PE-RZ復調部を含むBCA再生部820により、ID815、第1暗号鍵816、第2暗号鍵817、接続アドレス818のデータが再生される。パスワードをもらうためには、パスワード発行センター821のサーバーである第2コンピュータ821aの接続アドレス818へ通信部822を介してインターネット等のネットワーク823経由で接続し第2コンピュータ821aへIDを送信する。

【0018】ここで、暗号通信の手順について述べる。第2コンピュータ821aはユーザーの再生装置819からのID815を受信する。すると“モール”や“電

子商店”とよばれるパスワード発行センター821の第2コンピュータすなわちサーバー821aは暗号鍵データベースDB824をもつ。このデータベースにはこのディスク固有のIDもしくはIDの第1暗号鍵816に対応する復号鍵である秘密鍵、つまり第1暗号鍵825とIDの表が収容されている。従ってサーバーは受信したIDをもとに第1暗号鍵825を検索することが出来る。こうして第1コンピュータから第2コンピュータ821aへの暗号通信が成立する。この場合、第1暗号鍵と第1復号鍵は公開鍵暗号ではなく、共通鍵暗号の共通鍵なれば同じ鍵となる。

【0019】利用者はディスク801の中に、例えば、1000本収納されている暗号化されたコンテンツの1部、例えばコンテンツ番号826がnのコンテンツを利用したい場合、コンテンツ番号826つまりnを第1暗号鍵816である公開鍵を用いて、公開鍵暗号関数から構成される第1暗号エンコーダ827で、暗号化した暗号を第2コンピュータ821aに送信する。第2コンピュータ821a側では前述のようにこの暗号を復号するための第1復号鍵825を検索し知っている。従ってこの暗号を確実に平文化できる。こうしてユーザーの発注情報のプライバシーは暗号により守られるという効果がある。

【0020】この場合第1暗号鍵816として公開鍵暗号の秘密鍵を用いて署名してもよい。この方法は“デジタル署名”と呼ばれる。詳しい動作の説明は、暗号の専門書例えば、“E-Mail Security by Bruce Schneier 1995”の“Digital Signature”の項目等を参照されたい。

【0021】暗号通信にもどるとこの暗号は通信部822とネットワーク823を介して、パスワード発行センター821の第1暗号デコーダ827に送られる。こうして、第1暗号鍵816と対になっている第1対暗号鍵825を用いて第1対暗号デコーダ827では、暗号が復号される。

【0022】この場合、公開鍵は特定の1枚のディスクしかもっていないため、第三者のディスクからの不正な注文は排除できる。つまり、1枚のディスクの認証ができるためこのディスクの持ち主のユーザー個人の認証ができる。こうしてこのコンテンツ番号nは特定の個人の注文であることが証明されるため、第三者の不正な注文は排除できる。

【0023】この時公開鍵816を秘密にしておけば、この手法でクレジットカード番号等の高いセキュリティが要求される課金情報の送信にも技術的には用いることができる。しかし、通常“モール”と呼ばれる店では、セキュリティの保証がないため、電子決済ではユーザーの課金情報は扱わない。クレジットカード系と銀行系の課金センター828のみが、ユーザーの金融情報を取り

扱うことができる。現在、SET等のセキュリティ規格の統一が進められており、RSA1024bitの公開鍵暗号が使われ金融情報の暗号化が実現する可能性が高い。

【0024】次に本発明の場合の課金情報の暗号通信手順を示す。まず、BCA再生部820で再生された公開鍵暗号の第2暗号鍵817を用いて、個人のクレジットカード番号等の課金情報830は第2暗号エンコード831により、RSA等の公開鍵系暗号により、暗号化され、通信部822より第2コンピュータ821を介して第3コンピュータ828の暗号デコード832に送られる。この場合デジタル署名をする場合は第2暗号鍵817は秘密鍵829を用いる。

【0025】パスワード発行センター821の第2コンピュータ821aの暗号鍵の場合の手順と同様にして暗号鍵データベースDB824aよりIDもしくは第2暗号鍵817に対応する第2復号鍵829を検索し、これを用いて第2暗号デコード832において暗号化された課金情報を復号することができる。

【0026】なお第2暗号エンコード831で秘密鍵829を用いてデジタル署名すれば、第2暗号デコード832ではユーザーの署名を確認できる。こうして課金センター828は、ユーザーのクレジットカード番号や銀行カード番号や銀行パスワード等の課金情報をインターネットを使っても安全に入手することができる。インターネットのようなオープンなネットワークではセキュリティが問題となるが、このシステムでは、暗号通信用の暗号鍵（公開鍵）もしくはかつデジタル署名の秘密鍵がBCAに記録されているので、暗号通信もしくは認証が確実に行える。このため不正な第3者による不正課金と不正注文を防げるという効果がある。またディスク毎つまりユーザー毎に異なる公開鍵を用いることができるので通信の秘密性が向上し、ユーザーの課金情報が第3者に漏洩する可能性が減少する。

【0027】ここで、図6に戻り、パスワードの発行手順とパスワードによる解錠手順を説明する。パスワード発行センター821では、IDとユーザーが解錠したいコンテンツ番号とユーザーの使用許可期間を示す時間情報、の3つの情報に基づき、公開鍵暗号等の演算式を用いたパスワード生成部834でパスワードを生成し、第1コンピュータ909へ送信する。最も簡単な構成例を述べると、第2コンピュータではn番目のコンテンツの暗号を解除する復号鍵ディスクIDと時間情報を混合した情報を公開鍵暗号の公開鍵で暗号化し、これを解く秘密鍵を混合したn番目のパスワード834aをパスワード生成部834で作成し、第1コンピュータ909へ送信する。第1コンピュータは上述のn番目のパスワードを受信し、秘密鍵でディスクIDと時間情報とn番目のコンテンツの復号鍵を復号する。ここで、ディスクより再生したBCAのID835aと現在の第2時間情報8

35bと許可されたID833aと第1時間情報833を照合して一致するかをパスワード演算部836は演算する。もし一致すれば、許可し、n番目の復号鍵836aを暗号デコード837へ出力し、n番目のコンテンツの暗号837aが復号され、n番目のコンテンツ838が出力される。出力される期間は第1時間情報833と第2時間情報835bが一致している間だけに制限される。第1コンピュータ909側では、IDとパスワード835と現在の時間を示す時計836bからの時間情報の3つを情報をパスワード演算部836で演算し、IDと時間情報が正しければ、正しい復号鍵が演算結果として出力されるので、n番目の暗号が暗号デコード837で復号もしくは、デスクランブルされ、n番目のコンテンツ838の平文データもしくは、デスクランブルされた映像信号もしくはオーディオ信号が出力される。

【0028】この場合、時計836bの第2時間情報835bがパスワードの第1時間情報833と一致しないと暗号が正しく復号されないで再生はされない。時間情報を用いると、レンタル利用の際に3日間だけ映画を再生できるといった時間限定型のレンタルシステムに適用することが可能となる。

【0029】図6ではブロック図を用いて手順を説明したが、この手順のフローチャートは図16～図23を用いて後で説明する。

【0030】次に暗号鍵の容量についての工夫を述べる。こうして図7(a)に示すようにBCAに第1暗号鍵816と第2暗号鍵817の双方を入れることにより、“モールド”との商品取引と、“課金センター”との間の代金決済の2つのセキュリティが保たれるという効果が得られる。

【0031】この場合、課金センターとのセキュリティに関してはSET等の規格統一が予定されており、RSA1024つまり、128bytesの暗号鍵が、第2暗号鍵領域817aに収容されることになる。すると、BCAは188bytesしかないため、“モールド”との取引の暗号鍵用には60bytesしか残らない。20バイトの大ききでRSA1024の128バイトと同程度のセキュリティをもつ暗号関数として楕円関数公開鍵暗号が知られている。

【0032】本発明では、第1暗号鍵領域816aに楕円関数を用いている。楕円関数はRSA1024と同等のセキュリティが20バイトで得られる。このため、楕円関数を用いることにより188バイトのBCA領域に、第1暗号鍵816と第2暗号鍵717の双方が収容できるという効果がある。

【0033】以上述べたように、BCAを光ROMディスクに適用することにより、ディスク固有のID番号、第1と第2暗号鍵、接続のアドレスが記録できる。この場合インターネットを利用した場合に、自動的にモールドに接続され、コンテンツの暗号解除による商品流通と、

商品購入の認証と秘密保持、代金決済時の認証と機密性の保持等のセキュリティがBCAに暗号鍵が記録されたディスクを配布するだけで、実現する。このため本発明の暗号通信の方法により、従来のようなIDや、暗号鍵をユーザーへ配布するためにICカードやフロッピーや手紙を用いるという作業がセキュリティを落とすことなしに省略でき合理化できるといふ大きな効果がある。またインターネットの接続アドレスであるURLは固定ではなく、変更される。原盤にはURLが記録されており、このURLに接続すればよいが、変更された時原盤を変更するのは、時間的コスト的に効率が悪い。BCAに変更されたURLを記録しておき、BCAより接続アドレス931が再生された場合のみ原盤の接続アドレスよりBCA接続アドレス931を優先して接続すれば、原盤を新規に作成することなく、変更された接続アドレス931に接続されるという効果がある。

【0034】図6ではBCAに公開鍵の第1号鍵と公開鍵の第1号鍵を記録した場合を示した。

【0035】図8では、BCAに公開鍵の第1暗号鍵816と秘密鍵の第3復号鍵817aの2つを記録した場合と暗号鍵を発生させて暗号通信する場合の2種類の実施例を示す。図6と同様の手順であるため、違うのみを述べる。まず、プレス工場では、第1暗号鍵816と第3復号鍵817aがBCAに記録される。第3復号鍵817aは課金センターからの公開鍵で暗号化された暗号の受信に用いる。この場合、受信のセキュリティが向上するという効果がある。

【0036】まず、図8を用いて暗号鍵を生成するより具体的な暗号通信の例を説明する。第1暗号鍵816は公開鍵なので、受信用の第3復号鍵817aをBCAに記録する必要がある。一方BCAは容量が少ない。又公開鍵は処理時間を要する。そこで、図8では第1コンピュータ836で乱数発生器等で暗号鍵生成部838aで公開鍵の暗号鍵/復号鍵の対、又は共通鍵を生成する。共通鍵の例を述べる。共通鍵K838を第1暗号鍵816と第1暗号エンコード842で暗号化し、第2コンピュータ821aへ送る。第2コンピュータでは主復号鍵844を用いて、主暗号デコード843で、この暗号を平文化して共通鍵K838aを得る。双方が共通鍵Kをもつので、第2暗号エンコード842aと第2暗号デコード847aで共通鍵Kを渡すことにより、店からユーザー、つまり第2コンピュータ821aから第1コンピュータ836への暗号通信ができる。当然共通鍵Kを第2暗号エンコード827aと第2暗号デコード845aに渡すことにより、ユーザーから店つまり第1コンピュータ836から第2コンピュータ821aへの暗号通信も可能となる。公開鍵である第1暗号鍵をBCAに記録し、共通鍵を生成する方式の効果を述べる。まず、第1暗号鍵の記録だけでよく復号鍵の記録が省略できる。従ってBCAの少ない容量を減らすことがない。次にBC

Aに復号鍵が記録されているので、セキュリティが向上する。共通鍵の場合、毎回鍵を変えればよい。

【0037】演算時間が短いため、処理時間が少なくて済むという効果がある。この場合暗号鍵生成部838aが共通鍵ではなく、公開鍵の暗号鍵と復号鍵の一对を生成した場合暗号鍵を第2コンピュータ821aへ暗号送信し、第2暗号エンコード842aの暗号鍵として用い、復号鍵を第2暗号デコード847の復号鍵として用いれば処理時間は長くなるが共通鍵に比べてよりセキュリティを高めることができる。処理するCPUの性能が高い場合は公開鍵を使う方が望ましい。公開鍵を新たに生成する場合は、BCAには第1暗号鍵の公開鍵しか記録されないため、セキュリティの問題発生しない。BCAの容量も消費されない。また暗号鍵を変更する必要がないためメンテナンスも容易となる。

【0038】今度はパスワード発行センター821の第2コンピュータ821aで共通鍵K838aを定義した場合、共通鍵を第3暗号鍵839を用いて第3暗号エンコード840で暗号化し、パソコン836へ送信する。パソコン836側ではBCAより再生した秘密鍵である第3復号鍵837を用いて、第3暗号デコード841で平文化することにより、共通鍵K838bを得る。この場合、秘密鍵である第3復号鍵817aはこのユーザーしかもっていないので、センターからユーザーへの通信の内容が第三者に漏洩することは防止されるという効果がある。この場合のフォーマットを図7(b)に示す。第3復号鍵839bは積円関数を用いた20バイトでよいからBCAに収容できる。

【0039】次に図9を用いて、暗号化ディスクにBCAを用いて原盤作成費用を削減する実施例を説明する。

【0040】n個例えば、1000本の平文のコンテンツ850があると、各々1～m番目の暗号鍵851を用いて暗号エンコード852で暗号化する。この暗号化された第1～m番目のコンテンツ853と1～m番目のコンテンツの復号プログラム854aと第2暗号を復号するプログラムである第2暗号デコード861aは、原盤に凹凸のビットとして記録された後、1枚の基板に成形され反射膜を形成した後、2枚の基板が貼り合わせられて、光ディスク801aが完成する。この時、ディスク1枚目に異なるディスク固有の識別情報、いいかえるとID855とn番目、例えば1番目のコンテンツを解読するパスワードや復号鍵等の復号情報854を第2暗号エンコード860で暗号化した第2暗号を予めBCAに記録する。すると、再生装置ではBCA再生部820より第2暗号が再生される。BCA以外の通常の記録データが再生されるデータ再生部862よりは第2暗号デコード861が再生されるので、これを用いて第2暗号を復号し、ID855aと第n番目のパスワード854aが再生される。暗号デコード855bでは、データ再生部862より再生したn番目のコンテンツの復号プログラ

ム854aを用いて、ID855aとパスワード854aを用いて第1暗号を復号し、n番目のコンテンツの平文855cと識別情報855aを得る。パソコンの場合はハードディスク863にコンテンツとIDは記録される。このID855aは、プログラム起動時にネットワーク上に同じIDがないかをチェックし、ネットワークプロテクションを動作させるので、ソフトの不正インストールが防止できるという副次的効果がある。つまり、原盤1枚に暗号化した1千本のコンテンツを入れ、特定のソフトに対応するパスワード等の復号情報を記録しておけば、実質的に特定の1本のコンテンツの光ROMディスクを作成したのと等価となる。1枚の原盤で1000種類のソフトの原盤をカッティングしたのと同じ効果が得られ、原盤作成費用と手間が削減できるという効果がある。

【0041】図10ではRAMディスクに、コンテンツを記録する際にBCAを用いて暗号化する手順を述べる。まず、RAMディスク856よりBCA再生部820により、BCAのデータを再生し、ID857を出力し、インターフェース858a、858bとネットワークを介して、暗号化部859に送る。暗号化部859ではコンテンツ860をID857を含む鍵で暗号エンコーダ861において暗号化もしくは映像音声信号のスクランブルを行う。暗号化されたコンテンツは記録再生装置に送られ記録回路862によりRAMディスク856に記録される。

【0042】次に、この信号を再生する時は、データ再生部865により、主データの復調を行い、暗号化された信号を再生し、暗号デコーダ863において、復号が行なわれる。この時、RAMディスク856のBCA領域から、BCA再生部820により、ID857を含む情報が再生され、暗号デコーダ863に鍵の一部として送られる。この時、正規にコピーされた場合はRAMディスクに記録された暗号の鍵は正規のディスクIDであり、RAMディスクのIDも正規のディスクIDであるため、暗号の復号もしくはデスクランブルが行なわれ、第n番目のコンテンツの平文864が出力される。映像情報の場合はMPEG信号が伸長されて、映像信号が得られる。

【0043】この場合、暗号化はディスクIDを鍵として、ディスクIDは世の中に1枚しか存在しないため、1枚のRAMディスクにしかコピーできないという効果が得られる。

【0044】ここで、もしこの正規のRAMディスクから、別のRAMディスクにコピーした場合、最初の正規ディスクIDであるID1と、別の不正のRAMディスクのディスクIDであるID2とは異なる。不正のRAMディスクのBCAを再生するとID2が再生される。しかし、コンテンツはID1で暗号化されているので、暗号デコーダ863においてID2で解鍵しようとして

も、鍵が異なるため、暗号は復号されない。こうして、不正コピーのRAMディスクの信号が出力されず、著作権が保護されるという効果がある。本発明はDiskID方式での正規に1回だけコピーされた正規のRAMディスクはどのドライブで再生しても、暗号が解錠されるという効果がある。ただし、暗号化部859はセンターのかわりに暗号エンコーダを搭載したICカードでもよい。

【0045】図11のブロック図と図12のフローチャートを用いて、コピー防止方法を述べる。ステップ877aでインストールプログラムを動作させる。ステップ877bで貼り合わせた光ディスク801より、BCA再生部820より副情報のIDが出力される。ステップ877dでデータ再生部865より主情報よりコンテンツとネットワークチェックソフト870が再生される。コンテンツとID857はHDD872に記録される。ステップ877cで不正に改ざんされないようID857は特定の秘密の暗号演算を行い、HDD857にソフトIDとして記録される。こうして、パソコン876のHDD8572にはコンテンツとともにソフトID873が記録される。ここで図11のステップ877fのプログラムを起動する場合を述べる。プログラムを起動する時は、ステップ877gにおいて、HDD872のソフトID873を再生し、インターフェース875を介して、ネットワーク876の上の別のパソコン876aのHDD872aの中のソフトID873aをチェックする。ステップ877hで他のパソコンのソフトID873aと自分のソフトID873が同一番号であるかをチェックし、同一番号である場合は、ステップ877jへ進み、パソコン876のプログラムの起動を中止するか画面上に警告メッセージを表示する。

【0046】他のパソコンのソフトID873aが同一番号でなかった場合は、少なくともネットワーク上にはコンテンツを複数台にインストールした形跡はないため不正コピーはないと判断し、ステップ877kへ進み、プログラムの起動を許可する。この場合、他のパソコンへネットワークを介してソフトID873を送信してもよい。このパソコンでは各パソコンのソフトIDの重複をチェックすれば不正インストールが検出できる。不正があれば、該当するパソコンに警告メッセージを送る。

【0047】こうして、BCAにIDを記録し、ネットワークチェックプログラムをビット記録領域に記録することにより、同一ネットワーク上の同一IDのソフトの複数インストールを防止できる。こうして簡便な不正コピープロテクトが実現する。

【0048】図13のように白色の材料からなる書き込み可能な書き込み層850を塗布することにより設けることにより、文字を印刷したりペンでパスワード等を書き入れることができるだけでなく、書き込み層850が厚くなるため光ディスクの基板の損傷を防ぐという効果



も得られる。この書き込み層850の上のBCA領域801aにトリミングで記録されたBCAデータ849の一部であるディスクID815を平文化し英数字に変換した文字851と一般バーコード852を印字することにより、販売店やユーザーがBCAを再生装置でよみとることなく、POSのバーコードリーダーや視認でIDの確認や照合ができる。視認できるIDはユーザーがパソコン経由でIDをセンターに通知する場合は不要である。しかしユーザーが電話でIDをセンターに口頭で伝える場合は、BCAのIDと同じIDがディスク上に視認できる形式で印刷することにより、ユーザーがIDを目でよみとれるのでパソコンにディスクを挿入することなしにIDをセンターに伝えることができる。図13のフローチャートで光ディスクの製造ステップを説明する。ステップ853dで、原盤よりディスクの成形を行い、ビットの記録された基板を作成する。ステップ853eでアルミ反射膜を作成する。ステップ853fで2枚のディスク基板を接着剤で貼り合わせ、DVDディスク等を完成させる。ステップ853gでスクリーン印刷のラベル印刷をディスクの片面に行う。この時バーコードで原盤に個々の識別情報を記録する。ステップ853hでPOS用バーコードのフォーマットでディスク1枚ごとに異なるID等の識別情報をインクジェットバーコード印刷機や熱転写型バーコード印刷機で印刷する。ステップ853iで、このバーコードをバーコードリーダーでよみ出し、ステップ853jで識別情報に対応したBCAデータをディスクの第2記録領域に印刷する。この製造方法であると、BCAを除くPOSバーコードを含む全工程を終えた後にディスク識別情報を確認した上で、BCAデータを記録する。BCAはディスクを再生しないと読めないが、POSバーコードは密度が低いので市販のバーコードリーダーでよみとれる。工場の中のあらゆる工程で、ディスクIDが識別できる。BCAトリミングの前にPOSバーコードでディスクIDを記録しておくことにより、BCAとPOSバーコードの誤記録がほぼ完全に防止できる。

【0049】このBCA方式で二次、三次記録もできるBCAの利用方法について述べる。図15に示すようにソフトメーカーでは、工程(2)で示すように海賊版防止マークと照合暗号を二次記録もできる。工程(2)ではディスク1枚ごとに異なるID番号やユーザーとの秘密通信用の暗号鍵を記録したディスク944bを作成しても良い。このディスク944c、944dはパスワードを入力しなくても再生できる。

【0050】別の応用として工程(3)では、暗号化やスクランブルしたMPEG映像信号等の情報をディスク944eに記録する。MPEGスクランブルの詳細い動作は説明を省略する。ソフト会社では工程(4)においてID番号とスクランブル解除情報を復号するためのサブ公開鍵をBCAで二次記録したディスク844fを作

成する。このディスクは単独では再生はできない。工程(5)では、販売店でディスクの代金を受け取った後にサブ公開鍵とペアになっているサブ秘密鍵でパスワードを作成し、ディスクに三次記録する。もしくはパスワードの印刷されたレシートをユーザーに渡す。このあと、ディスク844gはパスワードが記録されているためユーザーが再生可能となる。この方式を用いると、代金の支払われていないディスクを万引きしても映像のスクランブルが解除されないため正常に再生されないため、万引きが無意味になり減るという効果がある。

【0051】レンタルビデオ等の店では恒久的にパスワードをBCA記録すると万引きされた場合、使用されてしまう。この場合は工程(6)に示すように店でBCAをPOSバーコードリーダーでよみとりスクランブル解除のためのパスワードをステップ951gで発行し、ステップ951iでレシートに印刷し、ステップ951jで客に手渡す。客の方は、自宅でステップ951kでレシートのパスワードをプレーヤーにテンキーで入力する。ステップ951pで所定の日の間だけ再生される。ディスクの一部のソフトのパスワードのみを与えてレンタルした場合に、他のソフトをみない時は、電話で、そのソフトのパスワードをステップ951uで通知しステップ951kで入力することにより、ディスクの他のソフトを再生することができる。レンタルビデオ店の例を示したがパソコンソフト店で、暗号化したパソコンソフトを売った時に、POS端末でパスワードを印刷して渡しても良い。

【0052】図15の工程(5)(6)のセル販売店、レンタル店における動作を図14を用いてより具体的に説明する。セル販売店ではソフトメーカーから暗号やスクランブルがかかったディスク944fを受け取り、ユーザーからの入金を確認するとバーコード記録装置945よりディスク944fのID番号、サブ公開鍵のデータをPOS端末946経由でパスワード発行センター952に送信する。小規模なシステムの場合パスワード発行センター、つまりサブ公開鍵のサブ秘密鍵を含むシステムはPOS端末の中にあっても良い。パスワード発行センターはステップ951qでディスクID番号と時間情報を入力し、ステップ951sで演算を行い、ステップ951tで、サブ秘密鍵を用いて暗号化し、ステップ951gでパスワードを発行しネットワーク948とPOS端末846を介してBCAバーコード記録装置945にパスワードを送り、記録されたディスク944gが客に渡される。このディスク944gは、そのまま再生できる。

【0053】次にレンタル店やパソコンソフト店の場合、まず暗号やスクランブルの解除されていないROMディスク944fを店頭に陳列する。客が特定のROMディスク944fを指定した場合、うずまき型にスキャンする回転型の光学ヘッド953を内蔵した円形バーコ

ードリーダ950を手に持ち透明ケース入りのディスク900の中心におしつけることにより、ディスク944fの無反射部915による反射層のバーコードを読み取り、ディスクID番号を読み取る。ディスクIDの商品バーコードを図13の852のように入刷することにより通常のPOS端末のバーコードリーダで読み取ることが出来る。原盤に予め記録されたプレスされた円形バーコードから読み取っても良い。これらのディスクIDを含む情報はPOS端末946により処理され、料金がクレジットカードから決済されるとともに、前述のようにID番号に対応したパスワードがステップ951gにおいてパスワード発行システムから発行される。レンタル用途の場合、視聴可能な日数を制限するためステップ951tで用いたように日付情報を加えて、ディスクID番号を暗号化しパスワードを作成する。このパスワードの場合、特定の日付しか作動しないため、例えば3日間の貸し出し期間をパスワードの中に設定できるという効果がある。

【0054】さて、こうして発行されたデスクランブルのためのパスワードはステップ951iにおいて、貸出日、返却日、レンタルのタイトル料金とともにレシート949に印刷され客にディスクとともに渡される。客はディスク944jとレシート949を持ち帰り、ステップ951kでパスワードを図6の第1コンピュータ909のテンキー入力部954に力入することによりパスワード835はID番号835aと演算されて暗号デコード837を入力され、復号鍵を用いて平文化される。正しいパスワードである場合のみ暗号デコード837でプログラムのデータをデスクランブルし、映像出力を出力させる。

【0055】この場合、パスワードに時間情報が含まれている場合、時計部836bの日付データと照合し、一致した日付の期間、デスクランブルをする。なお、この入力したパスワードは対応するID番号とともにメモリ755の不揮発メモリ755aにストアされ、ユーザーは一度パスワードを入力すると2度と入力することなしにデスクランブルされる。こうして流通において電子的にディスクの鍵の開閉ができるという効果がある。

【0056】図16を用いてソフトが暗号データとして記録されたディスクのソフトの復号方法を詳しく説明する。

【0057】ステップ865は暗号データと個別IDのユーザーへの配布の全体フローを示す。まず、ステップ865aでは、1枚の原盤のROM領域に、秘密の第1暗号鍵で暗号化されたm<sub>1</sub>のデータと、暗号化されたm<sub>2</sub>のデータを復号するプログラムを記録する。ステップ865bでは、原盤より基板を成形し、反射膜を付加した2枚の基板を貼り合わせて完成ROMディスクを複数枚、作成する。ステップ865cでは、完成ディスクの書換できない副記録領域(BCAとよぶ)に、暗号化デ

ータの復号に必要な復号情報(プレスしたディスク毎に異なるディスク識別情報 and/or 暗号データの復号鍵)をROM領域と異なる変調方法で記録する。ステップ865dでは、ユーザーは配布されたディスクを再生し、希望する暗号化データnを選択し、復号処理を始める。ステップ865eで、ユーザーの第1コンピュータで、ROM領域から暗号化データと復号プログラムを再生し、副記録領域(BCA)から、復号情報を読み出す。ステップ865fで、オンラインで第2復号情報を得ない場合は図17のステップ871aで、ID等の復号の補助情報を画面上に表示する。ステップ871bで、ユーザーはIDに対応するパスワード等の第2復号を入力し、第1コンピュータに入力する。ステップ871cで、ディスク識別情報と第2復号情報と暗号化データnを用いて公開鍵系暗号関数の特定の演算を行う。ステップ871dで結果が正しければ、ステップ871fでn番目のデータが平文化され、ユーザーはデータnのソフトを動作させることができる。

【0058】次に図18のフローチャートを用いて、BCAを用いたインターネット等で必須な暗号通信の方法を述べる。ステップ868は、ユーザーへ通信プログラムと通信暗号鍵を配布する方法のルーチンである。まず、ステップ868aで、1枚の原盤のROM領域に少なくとも通信プログラムや接続情報を記録する。ステップ868bで、原盤より基板を成形し、2枚の基板を貼り合わせて完成ROMディスクを複数枚作成する。ステップ868cで、完成ディスクの書換できない副記録領域(BCA)に、プレスしたディスク毎に異なるディスク識別情報と暗号通信用暗号鍵を記録する。場合により第2コンピュータの接続アドレス、もしくは、かつ暗号通信用復号鍵をROM領域と異なる変調方法で記録する。ステップ868dで、ユーザーの第1コンピュータで、ROM領域から通信プログラムと暗号化プログラムを再生し、副記録領域から、ディスク識別情報と通信用暗号鍵を読み出す。図19に進みステップ867aで、BCA領域に接続アドレスがある場合は、ステップ867bで、BCA領域のURL等の接続アドレスに基づき第2コンピュータに接続し、接続アドレスがない場合はステップ867cのROM領域の接続アドレスのコンピュータに接続する。ステップ867dで、送信データが入力され、ステップ867eで、BCA領域に暗号通信用暗号鍵がある場合はステップ867gでBCA領域の暗号通信用暗号鍵を用いて、送信データを暗号化し、第3暗号を作成する。また、ない場合はステップ867fでROM領域又はHDDの暗号通信用の暗号鍵を用いてデータを暗号化し、第3暗号を作成する。

【0059】次に図20では第2コンピュータ910から受信した暗号の復号鍵の生成ルーチンをステップ869で述べる。まず、第1コンピュータではステップ869aで、通信復号鍵が必要な場合は、ステップ869b

へ進み、BCAに通信用復号鍵があるかどうかをチェックし、復号鍵がない場合は、ステップ869cでROM領域から再生した暗号鍵/復号鍵の生成プログラムを用いてユーザーのキー入力もしくは乱数発生器のデータをROM領域から再生した第2暗号鍵を用いて第2通信暗号鍵/第2通信復号鍵を新たに生成する。ステップ869dで、“第2通信暗号鍵もしくは/かつユーザーデータ”をBCAに記録された通信暗号鍵とROM領域から再生して得た暗号化ソフトを用いて暗号化した第4暗号を作成する。ステップ869eで、第4暗号と、ディスク識別情報もしくは/かつユーザーアドレスを、ディスクから再生して得た接続アドレスの第2コンピュータに送信する。第2コンピュータの処理としては、ステップ869fで、第4暗号とディスク識別情報とユーザーアドレスを受信する。ステップ869gでは、復号鍵データベースから、ディスク識別情報と対になった通信復号鍵を選択し、これを用いて第4暗号を復号し、第2通信暗号鍵の平文を得る。ステップ869hで、第2通信暗号鍵を用いて、ユーザーデータの一部分を含むサーバーデータを暗号化した第5暗号を第1コンピュータへインターネット908で送信する。ステップ869iで、第5暗号（とディスク識別情報）を受信し前述の第2通信復号鍵とROM領域に記録された復号関数を用いて復号し、前述のサーバーデータの平文を得る。こうして、図20のステップ869の方式で、第1、第2コンピュータ間で双方向の暗号通信が実現する。

【0060】図21のステップ870では課金情報の受信ルーチンについて説明する。ステップ870aで、課金情報を入力する場合は、課金通信用の公開鍵暗号の第3暗号鍵を第2コンピュータへ要求する。ステップ870bでは、第2コンピュータが、第3コンピュータへ第3暗号鍵を要求する。やりとりのステップは省略するが、第3コンピュータ911はIDと第3暗号鍵を第2コンピュータ910へ送信する。ステップ870cで、第2コンピュータはIDと第3暗号鍵を受信し、ステップ870eで、第3暗号鍵を第2通信暗号鍵等を用いて暗号化した第7暗号を第1コンピュータへ送信する。第1コンピュータではステップ870fで、第7暗号を受信し、ステップ870gで、前述の第2通信復号鍵を用いて、受信した第7暗号を復号し、第3暗号鍵（公開鍵関数の公開鍵）を得る。ステップ870hでは、必要に応じて第3暗号鍵をHDDに記録する。これは次の送信時に利用する。ステップ870iで、クレジットカード番号や決済用パスワード等の機密値が高い課金情報を入力する場合は、ステップ870jで第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号を第2コンピュータ経由で第3コンピュータへ送る。第2コンピュータは、ステップ870kで第8暗号を受信し、第3コンピュータへ再転送する。第3暗号の復号鍵は金融機関である第3コンピュータ912しか持っていないため、第2

コンピュータの電子商店では解読できない。第3コンピュータではステップ870mで、暗号鍵データベースからディスク等の識別情報を用いて第3暗号鍵に対応した第3復号鍵を探しだし、公開鍵暗号の秘密鍵である第3復号鍵で第8暗号を復号し、課金情報の平文を得る。ステップ870nでは、ユーザーの信用情報や預金残高等の金融情報から、代金が回収できるかをチェックし、ステップ870pでは、調査結果を第2コンピュータへ通知する。第2コンピュータいゆる電子商店はステップ870qで代金の回収可能かどうかを判定して、不能と判断すれば、ステップ870rで、商品の発送と暗号ソフトを復号する鍵の送付をしない。代金回収可能と判断した場合、図16のような鍵提供システムの場合、ステップ870sへ進み、暗号ソフトの復号鍵つまり商品をインターネット908で、ユーザーの第2コンピュータに送信する。第1コンピュータでは、ステップ870tで、暗号ソフトの復号鍵を受信して、ステップ870uでn番目の暗号化ソフトの暗号を解除して、ステップ870wで、ソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

【0061】この図21のステップ870の方式は課金情報という高いセキュリティが要求される第3暗号鍵の公開鍵を第3コンピュータつまり、金融機関に、必要に応じて要求し発行させる。BCAに予め記録しておかなくてもよい。従って第3暗号鍵にRSA2048の256バイトのさらに強力なRSA系の暗号鍵をBCAの容量を消費することなしに用いることができるという効果がある。さらに全てのディスクのBCAに予め記録する必要がないので、第3暗号鍵の発行総数が少なくなり、第3暗号鍵の演算に要するコンピュータのCPUタイムが減る。また、第3暗号がBCAにないため、公開されないため、セキュリティが若干向上する。この場合のBCAの役割は、第1、2図のように、RSA1024クロードの暗号鍵による秘密通信ディスクの識別情報の記録である。BCAディスク1枚あれば、第2コンピュータとの暗号通信が実現するため効果は高い。

【0062】次に図22を用いて、BCAに通信暗号鍵と通信復号鍵の双方を記録した時の、暗号通信のステップ872を説明する。ステップ872gで、第1コンピュータ909ではBCAから再生して得た通信暗号鍵でユーザーデータを暗号化した第9暗号と、原盤作成時にROM領域に記録された基本識別情報と、BCA領域に記録されたディスク識別情報を第2コンピュータ910へ送信する。第2コンピュータでは、ステップ872bで、第9暗号とディスク識別情報と基本識別情報を受信する。ステップ872cで、復号鍵データベースからディスク識別情報と対になった通信復号鍵を検索し、第9暗号を復号し、ユーザーデータの平文を得る。ステップ872eで、ディスク識別情報に対応した第2暗号鍵を暗号鍵データベースから選別し、この第2暗号でサーバ

一データと図21で述べた手順で第3コンピュータから受信した第3暗号鍵を暗号化した第10暗号を第1コンピュータへ送信する。第1コンピュータではステップ872fで、第10暗号を受信し、ステップ872gで、BCAに記録された前述の通信用第2復号鍵を用いて、受信した第7暗号を復号し、サーバーデータと第3暗号鍵（公開鍵関数の公開鍵）の平文を得る。ステップ872hで必要に応じて第3暗号鍵をHDDに記録する。ステップ872iで課金情報を入力する場合は、ステップ872jへ進み、第3暗号鍵を用いて、上記課金情報を暗号化した第8暗号と第1暗号を第2コンピュータ経由で第3コンピュータへ送る。第2コンピュータでは、ステップ872mで、第11暗号を第3コンピュータへ再送信する。第3コンピュータでは、ステップ872mで、第3暗号鍵をデータベースからディスク等の識別情報と対になった第3暗号鍵を探しだし、第8暗号を復号し、課金情報の平文を得る。ステップ872nでは、ユーザーへの課金回収の可能性のチェックを行い、ステップ872pで調査結果を第2コンピュータへ送信する。第2コンピュータではステップ872qでユーザーが課金の回収が可能かどうかをチェックする。代金回収可能と判断した場合図16のような鍵提供システムの場合、ステップ872sへ進み、暗号ソフトの復号鍵、つまり商品をインターネットでユーザーの第2コンピュータに送信する。第1コンピュータではステップ872tで暗号ソフトの復号鍵を受信して、ステップ872uでn番目の暗号化ソフトの暗号を解除してステップ872wでソフトの平文を得る。こうして、コンテンツの鍵提供システムが実現する。

【0063】図22のステップ872の方式の効果の特長は、暗号鍵と復号鍵の双方がBCA領域に記録されているため、第2コンピュータからの受信に必要な復号鍵や暗号鍵の送信が必要ないという点である。BCAの容量は最大188バイトであるので、公開鍵等の暗号関数なら、RSA512バイトで64バイト2ヶで、128バイトで済むので記録できる。RSA512にグループの双方向の暗号化が可能となる。楕円関数なら図7に示したように7〜8ヶ収容できるため、効果はさらに高い。

【0064】図23を用いて、BCAに第1暗号鍵と第3暗号鍵を予め記録した場合の動作と効果について述べる。なお、図22のステップ872a〜872wと図23のステップ873a〜873wは、ほぼ同じ構成なので違うステップだけを説明する。

【0065】まず、課金情報等の金融情報セキュリティを守る第3暗号鍵がBCAに記録されているので、ステップ873eにおいて第2、第3コンピュータは第3暗号鍵の生成と送信は不要となる。ステップ873e、873f、873gにおいて第12暗号の送受信が行われる。また、ステップ873jにおいてはBCA領域か

ら第3暗号鍵を読み出し、ユーザーの課金情報を第2コンピュータ経由で第3コンピュータへ送る。図23の方法は、第3暗号鍵の生成、送受信が全く不要となるため、手順が簡単になるという効果がある。

【0066】さて、電子決済システムの場合、課金センターはクレジット開始と同様、通常、複数個存在する。従って、当然公開鍵である第3暗号鍵は複数個必要となる。図7(b)で説明したようにRSA暗号鍵を使うとRSA1024グレート以上つまり128バイト以上必要であるので、BCAの188バイトには1ヶしか第3暗号鍵17bは入らない。しかし、近年登場した楕円関数系暗号鍵（楕円暗号）は小容量でRSAと同等のセキュリティが得られる。近年ではRSA関数のRSA1024が金融情報のセキュリティの最低基準となっている。RSA関数だと128バイト必要であるが、同等のセキュリティを得るのに、楕円暗号であると、20〜22バイト程度で良いといわれている。従って図7

(c)に図示するように金融情報を取り扱う第3暗号を複数ヶ、最大7〜8つBCAに収容できる。楕円暗号を使うことにより、現実的に必須である複数の金融センターに対応した、BCA応用の電子決済システムが実現する。第3暗号に的を絞って説明したが、第1暗号鍵の公開鍵に用いても、複数の電子商店との間の高いセキュリティが保たれるため楕円暗号の効果は同様である。

【0067】次に図24を用いて、図10で説明したBCAを用いたRAMディスク記録再生装置に更に詳しく述べる。1つの実施例としていわゆるPay per ViewシステムにおけるRAMディスクへの記録手順を述べる。まず、CATV会社等のソフト会社は番組送信器883において、映画ソフト等のコンテンツ880を第1暗号鍵882を用いて第1暗号器において暗号化し、第1暗号900を生成し、各ユーザーのCATVデコーダの如きデコーダ886に送信する。デコーダ886側ではネットワークを介して鍵発行センター884へ特定の番組の要求を送ると、鍵発行センター884は、特定のソフトでかつ特定のデコーダのシステムID番号かつ特定の時間制限情報903に対するスクランブル解除キーの如き第1復号情報でかつ、RAMディスクへの記録許可カード901が含まれている第1復号情報885aを第1デコーダ886の第1復号部887へ送信する。第1復号部887はシステムID888と第1復号情報885aより、第1暗号900を復号し、映像信号の場合は、一旦デスクランブルされた信号がさらに別の暗号でコピー防止用のスクランブルされた信号が第3暗号出力部889から出力され、一般TV899で、元のTV信号がコピーガードされているが視聴できる。ここで、記録許可コード901aがNOの場合は、RAMディスク894に記録できない。しかし、OKの場合はRAMディスク894の1枚に限り記録できる。この方法を説明する。

【0068】デコーダ886では、ICカード902が挿入され、RAMレコーダのRAMディスク894のBCAをBCA再生部895が読み取りディスクID905がICカード902に送られる。ICカード902はディスクIC905とデコーダ886から得た現在の時間情報904と記録許可コード901aをチェックし、第3暗号出力部889と双方向でシェイクハンド方式のコピーチェック907を行い、記録許可コードとコピーチェックがOKならICカード902の中の第2副暗号器891は第2暗号鍵906を発行する。第2暗号器890において、第3暗号は再暗号化されて特定の1枚のディスクのディスクIDでコンテンツ880が暗号化された第2暗号が生成され、RAMレコーダ892に送られ記録手段893において8-15や8-16変調を用い、第1変調部により変調され、レーザにより、RAMディスク894の第1記録領域894aに第2暗号912が記録される。こうしてRAMディスク894のデータは特定のディスクIDの番号で暗号化される。

【0069】次にこのディスクを通常の再生手段896で再生信号を8-16変調の第1復調部896aで復調するとコンテンツの第2暗号が出力される。第2復号器897は複数の第2暗号鍵898a、898b、898cをもつ。これは各CATV局等の番組供給会社毎に異なる各々のICカードの暗号鍵に対応した復号鍵をもつことになる。この場合、デコーダ886もしくはICカード902の復号鍵識別情報は記録時に第1記録領域894aに記録されている。再生装置では、第1記録領域894aから復号鍵識別情報913をよみ出し、復号鍵選択手段914により復号鍵898a~898zのうちからを元に各々の暗号鍵に対応した、第2復号鍵898aを自動的に選択し、ディスクID905aを一つの鍵として、第2暗号は第2復号器897において復号される。特定の復号鍵の入ったICカードを用いてもよい。映像の場合TV899aにてデスクランブルされた正常な映像が得られる。

【0070】図24のシステムでは、各ユーザーの自宅のデコーダに挿入したICカードにディスクID905を送り、画像データ等を暗号化するので、ソフト会社883は各ユーザーに配信するコンテンツの暗号を個別に変える必要がない。従って、衛星放送やCATVのように大量の視聴者にペーパービューのスクランブル映像を放送する場合に、各ユーザー毎にRAMディスク1枚だけに記録することを許可することができるという効果がある。

【0071】図24のシステムで1枚のディスクに記録すると同時に、2枚目つまり他のディスクIDのRAMディスクに不正にコピーより記録しようとするBCAの場合2層ディスクを用いているのでディスクIDを改ざんすることができないため、同時に2枚目のディスクへの不正コピーは防止される。次に別の時間帯に擬

似的な記録許可コード901aや第3暗号をデコーダICカードに送信し、特定のディスクIDでデータは暗号化されている。別のディスクIDのRAMディスクに記録することが考えられる。こうした不正行為も、ICカードの中のデコーダ時間情報管理部902が鍵発行センター884の時間制限情報903やコンテンツの時間情報の時間とデコーダの中の時間情報部904aの現在の時間とを比較して、時間が一致しているかどうかをチェックし、OKならICカード902は第2暗号演算器990の暗号化を許可する。

【0072】この場合、第2暗号器890と第1復号部887が双方向でチェックデータを送信するシェイクハンド方式の時間チェック方式でもよい。

【0073】シェイクハンド方式の場合、ICカードを含む第2暗号演算器890と、第1復号部887と第3暗号部889は双方向で、暗号データを確認しあう。このためコンテンツの送信時間と同一でない別の時間帯の不正コピーは防止される。

【0074】こうして各ユーザーのもつデコーダ886においては世の中に1枚しか存在しない特定のディスクIDのRAMディスク894の1枚のみに、ソフト会社のコンテンツが記録される。そして、このディスクはどのRAMディスク再生機でも再生できる。図24の方式でRAMディスクに記録する場合でもソフト会社の著作権が守られるという効果がある。

【0075】なお本文の図の説明では、暗号エンコーダで暗号化、暗号デコーダで復号化を説明したが、実際はCPUの中のプログラムである暗号アルゴリズム及び復号アルゴリズムを用いる。

【0076】

【発明の効果】このように、光ディスクのBCA領域にIDや暗号の暗号鍵や復号鍵を予め記録しておくことにより、暗号化されたコンテンツの暗号解除がより簡単な手順で実現する。また通信の機密性が従来の登録手続きなしで実現する。ネットワークチェックプログラムをコンテンツに収納しておくことにより、同一ネットワーク上の同一IDソフトの複数インストールを防止できる。このようにセキュリティ向上の様々な効果がある。

【図面の簡単な説明】

【図1】本発明の実施例の光ディスクの工程図

【図2】本発明の実施例のバブルスレーザによるトリミングの断面図

【図3】本発明の実施例のトリミング部の信号再生波形図

【図4】本発明の実施例の再生装置のブロック図

【図5】(a) 本発明のBCA部の再生信号波形図

(b) 本発明のBCA部の寸法関係図

【図6】本発明の実施例の暗号通信の方法とパスワードによる暗号鍵の方法を示した図

【図7】本発明のBCAのフォーマット図

【図8】本発明の実施例の暗号通信の方法とパスワードによる暗号解鍵の方法を示した図

【図9】本発明の実施例のコンテンツ部分を使用許可したディスクの動作手順図

【図10】本発明の実施例のRAMディスクにBCAを記録した場合のブロック図

【図11】本発明の実施例の不正コピー防止方式のブロック図

【図12】本発明の実施例の不正コピー防止のフローチャート

【図13】本発明の実施例のBCAに商品バーコードを印刷した光ディスクの上面図と断面図

【図14】本発明の実施例のBCA付ROMディスクとPOS端末を用いたPOS決済システムのブロック図

【図15】本発明の実施例のプレス工場とソフト会社と販売店の暗号解除の流れ図

【図16】本発明の実施例のディスクID等を用いた暗号データの暗号化復号化ステップのフローチャート

【図17】本発明の実施例のディスクID等を用いた暗号データの暗号化復号化ステップのフローチャート

【図18】本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図19】本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図20】本発明の実施例のBCAを用いた通信暗号鍵の配布と暗号通信のフローチャート

【図21】本発明の実施例のBCAを用いた電子決済システムのフローチャート

【図22】本発明の実施例のBCAを用いた電子決済システムのフローチャート

【図23】本発明の実施例のBCAを用いた電子決済システムのフローチャート

【図24】本発明の実施例のBCAを用いた1枚のRAMディスクに記録制限する記録再生方法のブロック図

【符号の説明】

801 BCA付ディスク

802 固定鍵

803 暗号エンコーダ

804 記録手段

805 コンテンツ

806 ID

807 トリミング装置

808a 成形機

808b 反射膜作成機

808c 貼り合わせ機

809 完成ディスク

809a 片面ディスク

809b 片面ディスク

811 プレス場

813 固定鍵

814 BCA領域

815 ディスクID

816 第1暗号鍵(秘密鍵)

817 第2暗号鍵(秘密鍵)

818 接続アドレス

819 再生装置

820 BCA再生部

821 パスワード発行センター

822 通信部

823 ネットワーク

824 暗号鍵DB

825 第1復号鍵

826 コンテンツ番号

827 第1暗号デコーダ

828 課金センター

829 第2復号鍵

830 課金情報

831 第2暗号エンコーダ

832 第2暗号デコーダ

833 時間情報

834 パスワード生成部

835 パスワード

836 バソコン

837 第3復号鍵

838 共通鍵

839 第3暗号鍵

840 第3暗号エンコーダ

841 第3暗号デコーダ

842 主暗号エンコーダ

843 主暗号デコーダ

844 主復号鍵

845 第1暗号デコーダ

846 暗号エンコーダ

847 暗号デコーダ

849 BCAデータ

850 書き込み層

851 文字

852 一般バーコード

853 復号器

860 第2暗号エンコーダ

861 第2暗号デコーダ

862 データ再生部

863 ROM領域

864 追記領域

865 復号フローチャート

890 第2暗号演算器

894a 第1記録領域

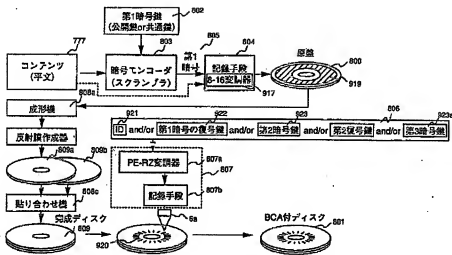
908 インターネット

909 第1コンピュータ

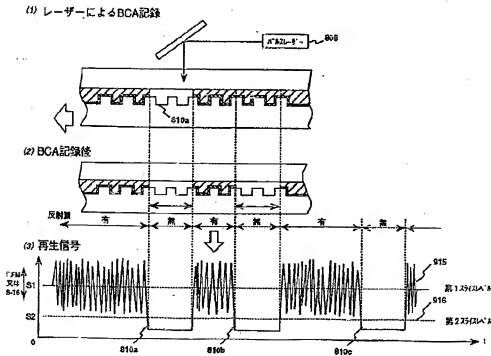
910 第2コンピュータ

- |               |               |
|---------------|---------------|
| 911 第3コンピュータ  | 921 ディスクID    |
| 912 第2暗号      | 922 BCAフラグ    |
| 913 復号鍵識別情報   | 923 CPU       |
| 914 復号鍵選別手段   | 924 コントローラデータ |
| 915 第1スライスレベル | 925 EFM復調     |
| 916 第2スライスレベル | 926 8-15変調復調  |
| 917 PE-RZ変調器  | 927 8-16変調復調  |
| 918 透明基板      | 928 第1復調部     |
| 919 第1記録領域    | 930 第2復調部     |
| 920 第2記録領域    | 931 接続アドレス    |

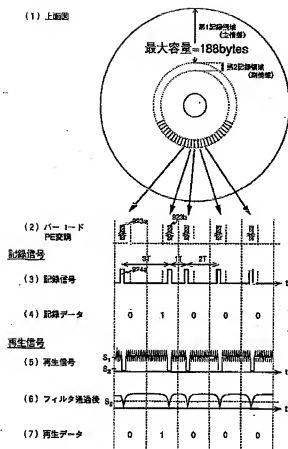
【図1】



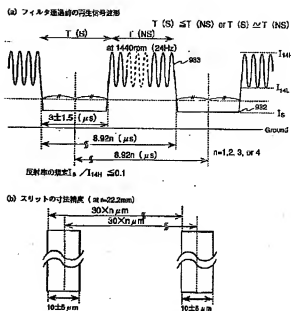
【図2】



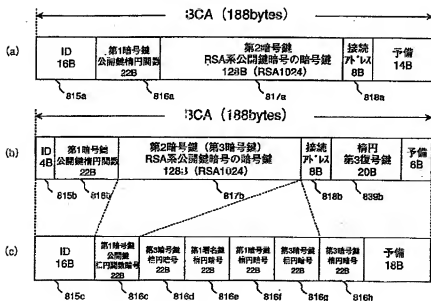
【图3】



【图5】



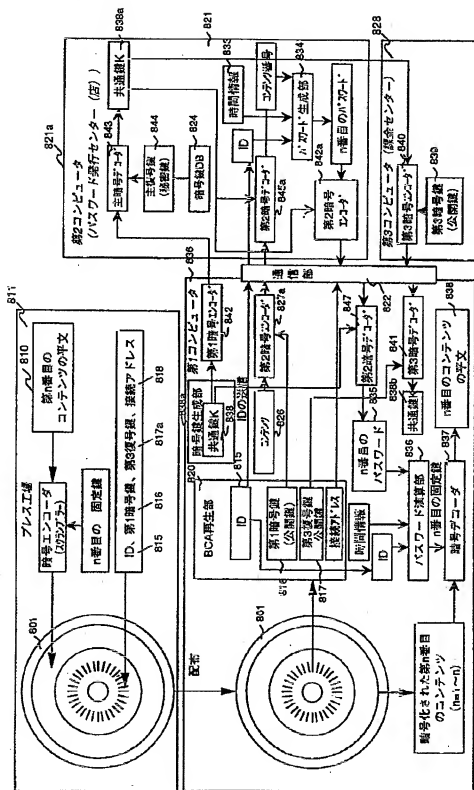
【图7】





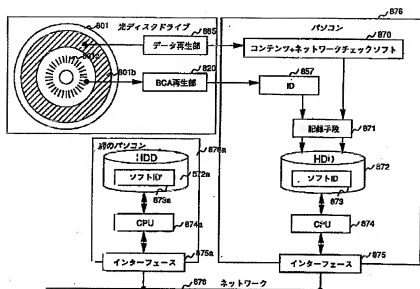




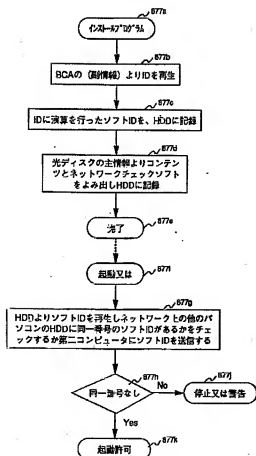




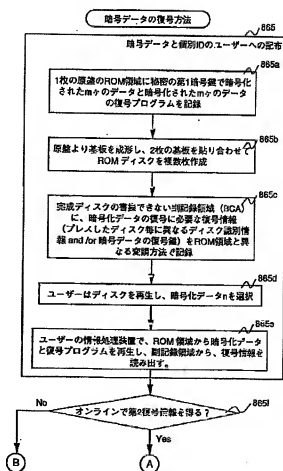
【図11】



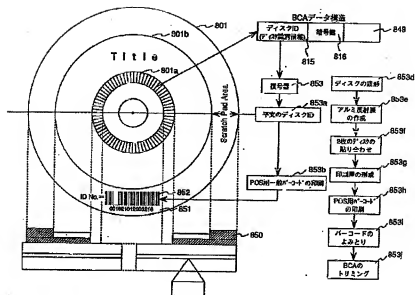
【図12】



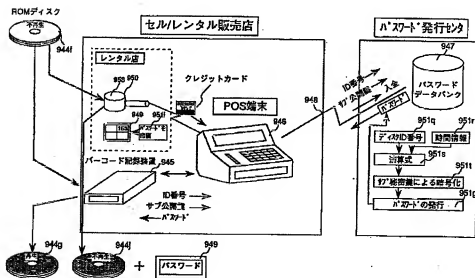
【図16】



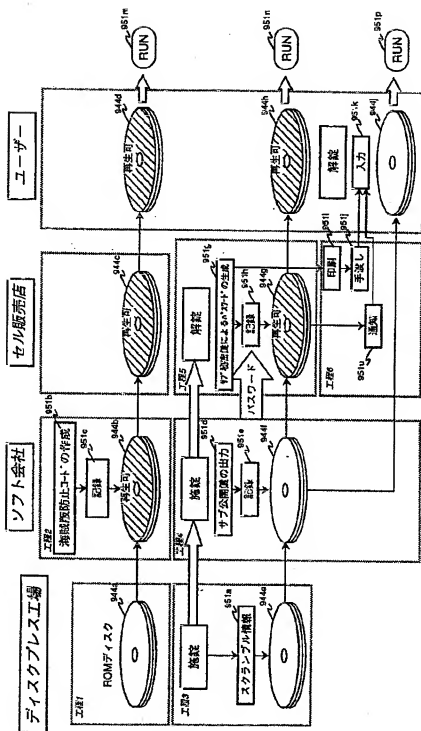
【图13】



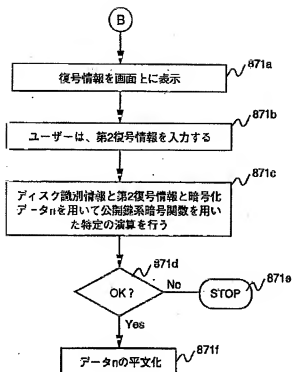
【图 14】



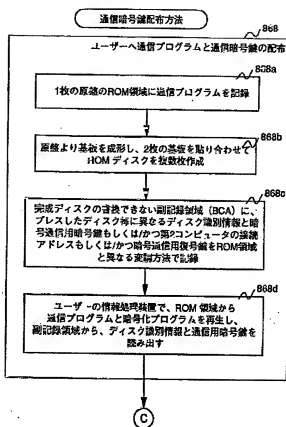
【図15】



【図17】

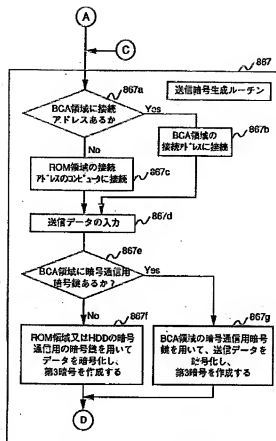


【図18】

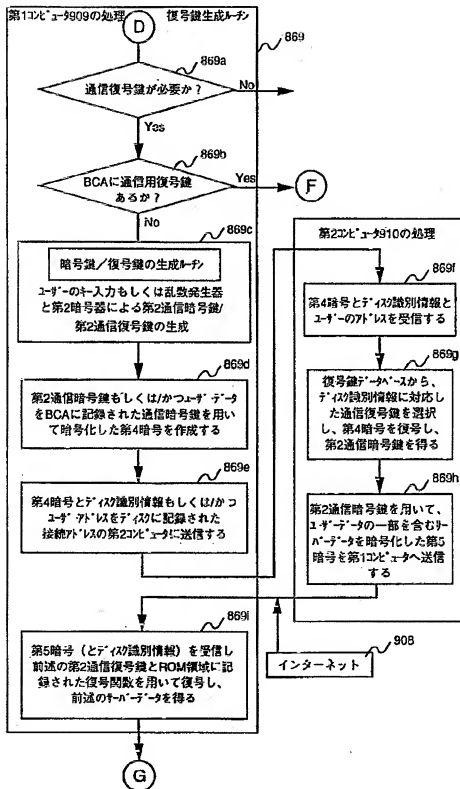




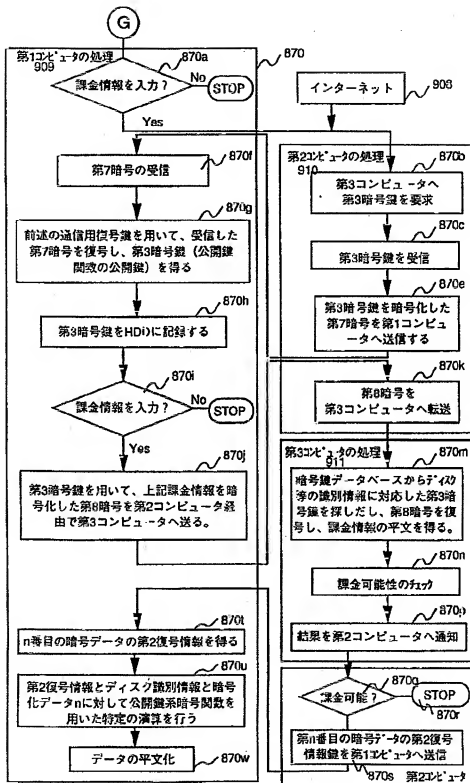
【図19】



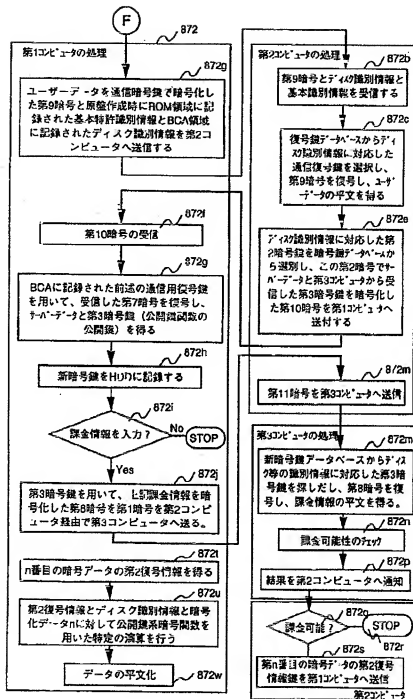
【図20】



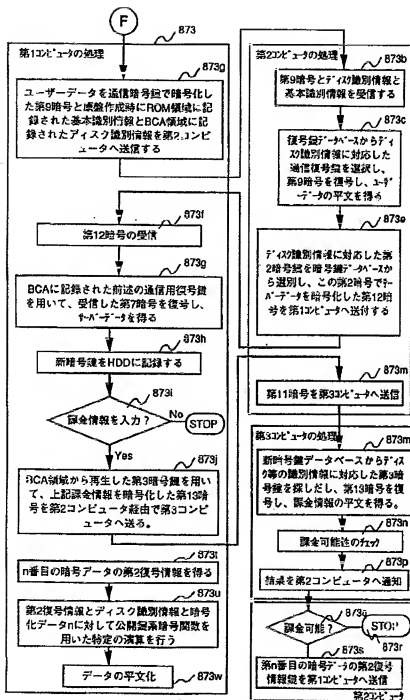
【図21】



【図22】



【図23】





(72)発明者 守屋 充郎  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72)発明者 竹村 佳也  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 5B017 AA03 AA06 BA07 BB09 BB10  
CA09 CA16  
5D044 AB01 BC03 CC06 DE50 DE52  
FG18 GK12 GK17 HH15 HL08  
5D090 AA01 BB02 CC04 CC14 DD05  
FF09 GG17 GG36  
5J104 AA16 NA32 PA14